Qualys Container Security

Comprehensive Security for the ever-changing Container Stack

Hari Srinivasan
Director Product Management, Qualys, Inc.

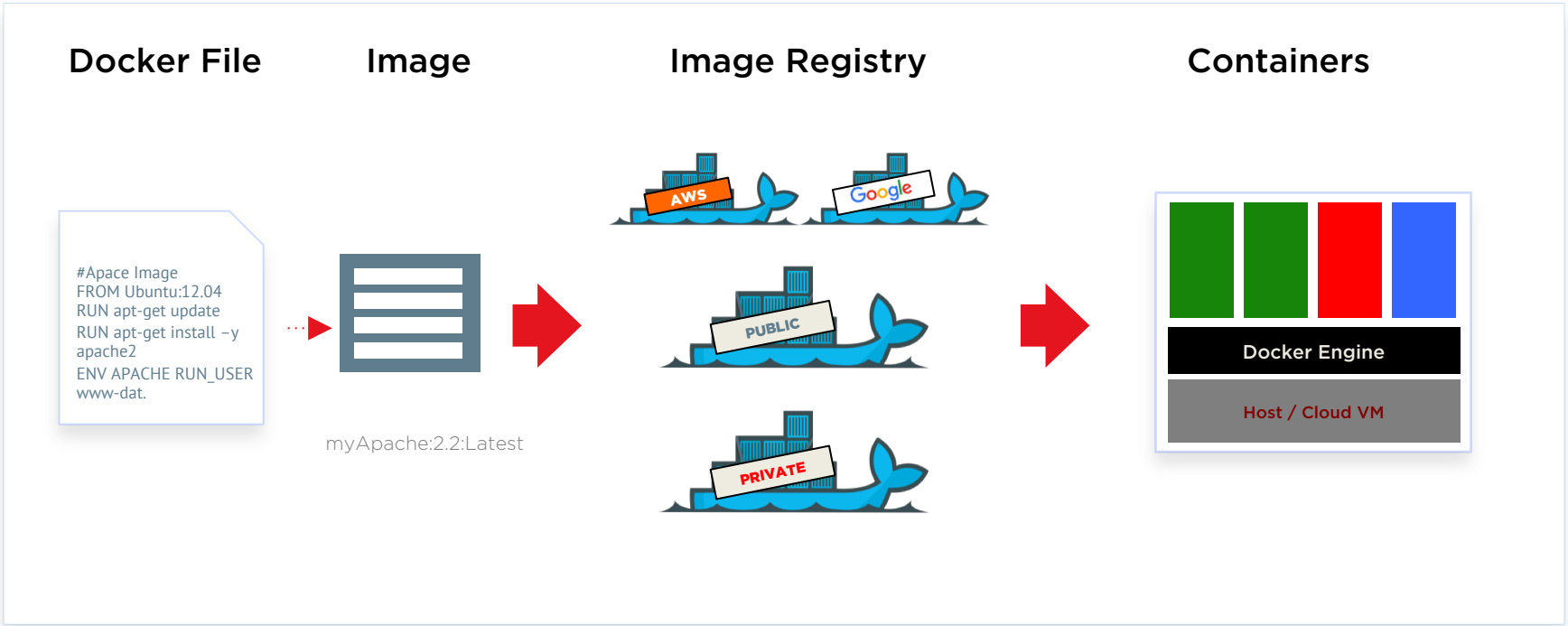
Everybody Loves Containers

Portability

Agility

Density

Container Components & Lifecycle



Container Platforms

On Premise

RED HAT® OPENSHIFT

Pivotal Container Service™

Cloud

Amazon ECS

Amazon EKS

Azure Container Service

Google Cloud Container Engine

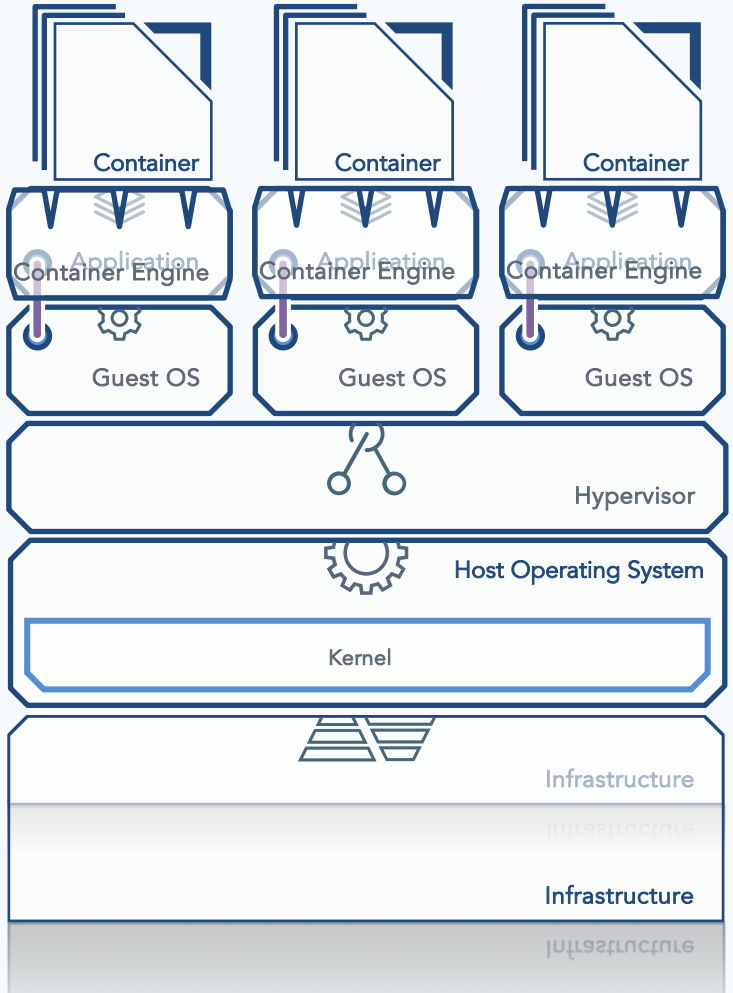
Qualys.

Container Deployments

Deployment Scenario #1

Use Case

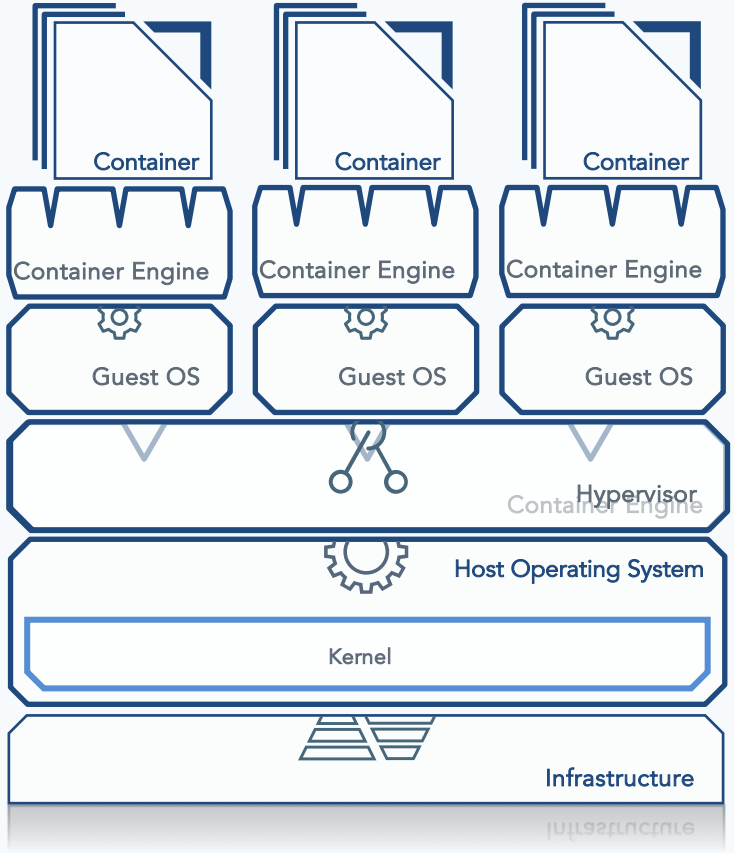
1. Shrinking infrastructure, as organizations continue migration to the cloud
2. Containers deployed within Virtual Machines
3. But organizations still have the overhead and costs of the hypervisor and virtual machines



Deployment Scenario #2

Use Case

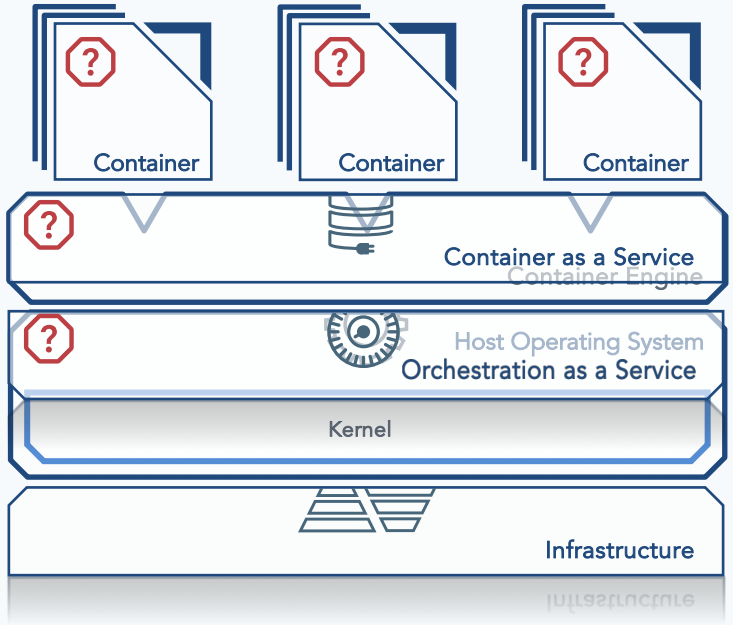
1. The orchestration battle ends with Kubernetes winning 80% of the market
2. But organizations struggle to scale their own Kubernetes clusters



Deployment Scenario #3

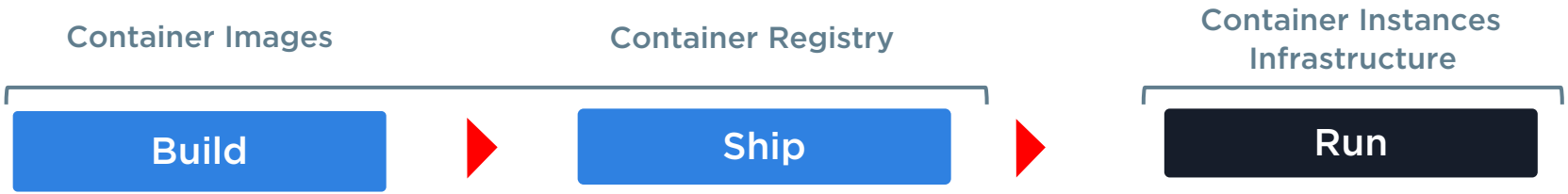
Use Case

1. Container-as-a-Service and Orchestration-as-a-Service adoption accelerate container adoption
2. Now where do you put security?



Container Visibility & Security Challenges

Container Lifecycle Challenges



What's in the images?

Vulnerabilities?

OSS license exposure?

Solution disruptive to my CI Pipeline?

Scanning report integrated with bug tracking?

Registry scanning?

Enforce compliance?

Vulnerability, package and license-based rules?

Vulnerability impact notifications?

How to protect host?

Container engine configured correctly?

Container orchestration configured correctly?

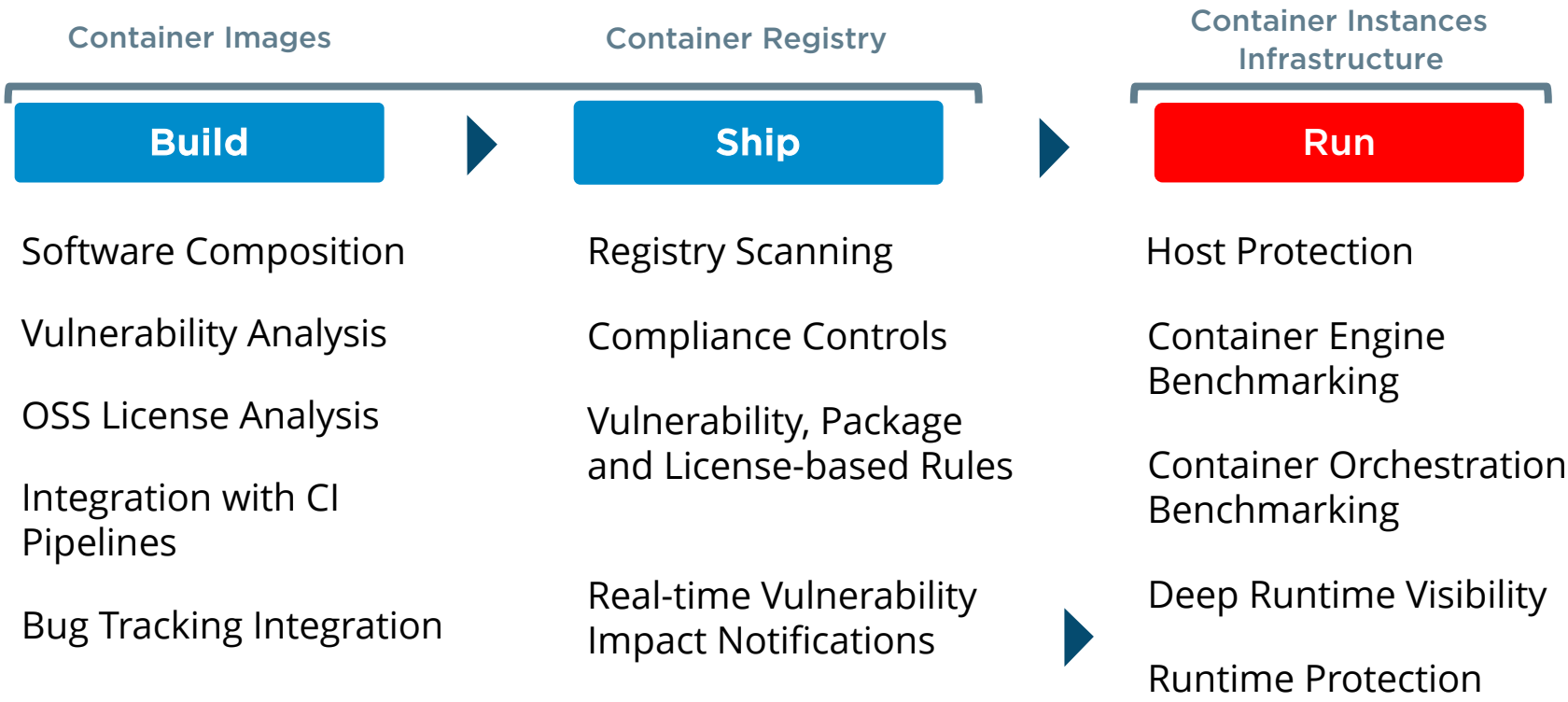
Runtime app visibility?

Runtime app protection?

Qualys.

Qualys Container Security

Qualys Container Security



Qualys Container Security

Key Uses

Visibility into your container projects

Identify Hosts with Containers. Inventory of images, containers. Search images with vulnerabilities, labels, tags, packages,.. Build custom widgets.

Secure the CI/CD pipeline

Integrate images, vulnerability scans into the build. FAIL builds, not allowing unsecure images to enter the stream

Scan Registry and block unauthorized images

Inventory and scan as new images are added to the registry. Block unapproved images from being spun up as Containers.

Container Runtime Visibility and Protection

Find what containers are running, know if the runtime got changed from images. Protect from changes or breakouts.

Use Case #1

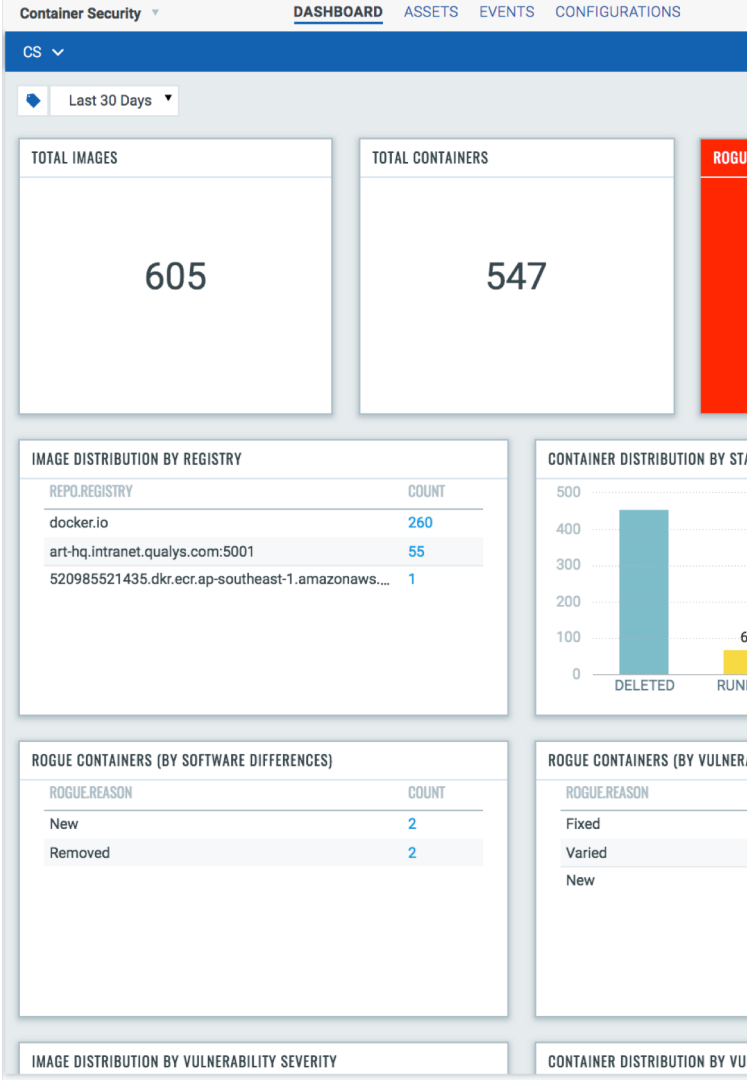
Visibility into your container projects

Overview Dashboard

Inventory & security posture widgets

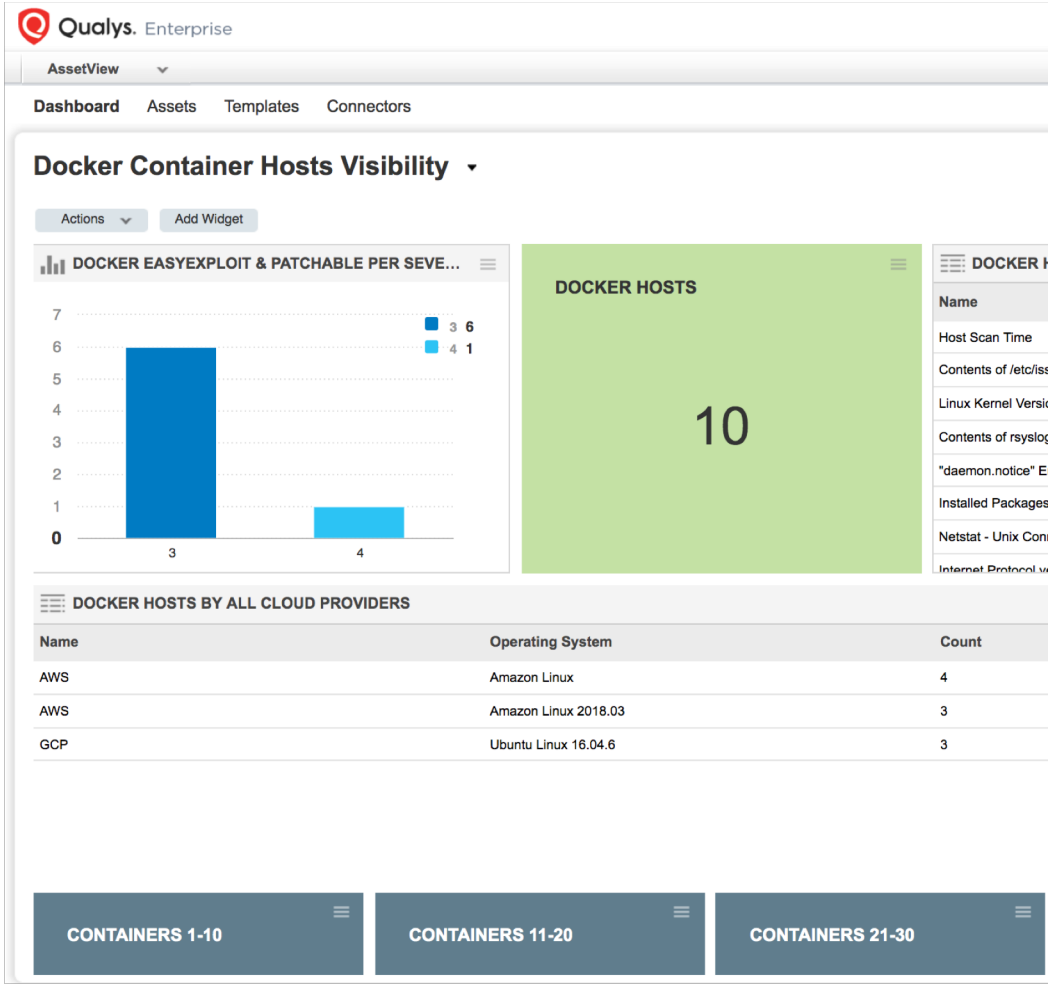
- Container Hosts
- Count of images, containers
- Containers by state
- Vulnerable images

Personalize and add custom widgets

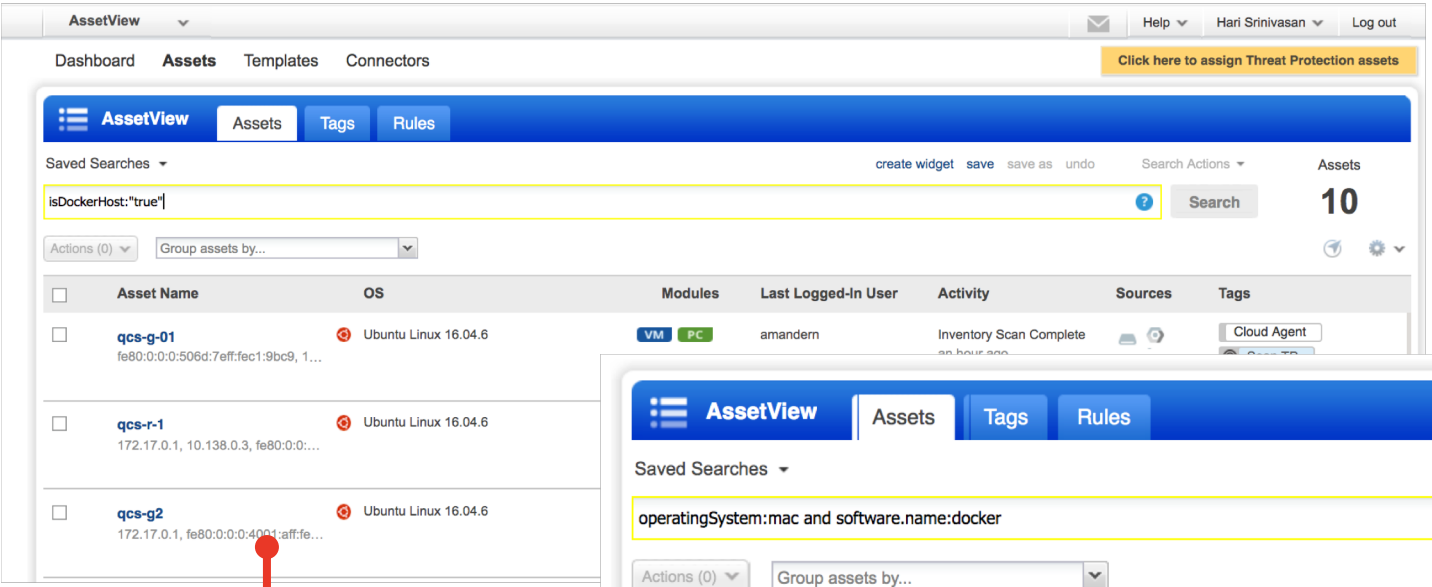


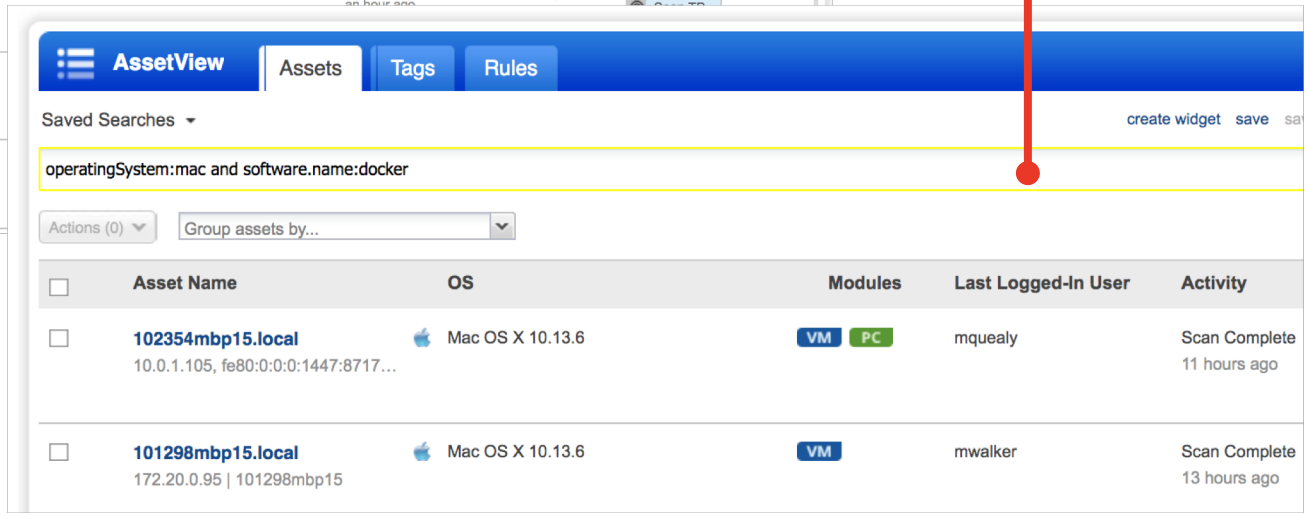
Know where your Containers are?

- Inventory of all Container Hosts across your datacenters, public clouds, laptops,..
- Know how the host vulnerabilities, exploits affect your container environments



Know where your Containers are?





Developer Mac laptops

Servers – Datacenter, Clouds, etc..

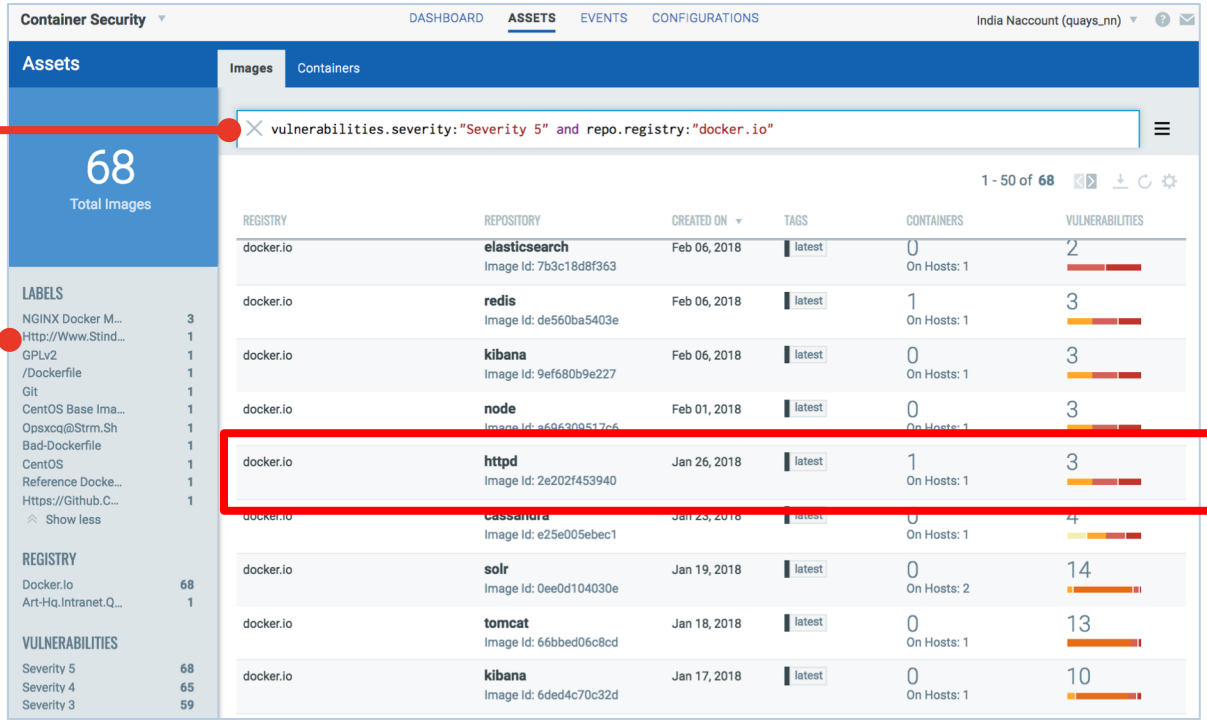
isDockerHost: "true" and provider: AWS/Azure/GCP

Image Inventory and Smart Searches

Search based on all attributes

Preset quick search filters

- Identify images by application labels



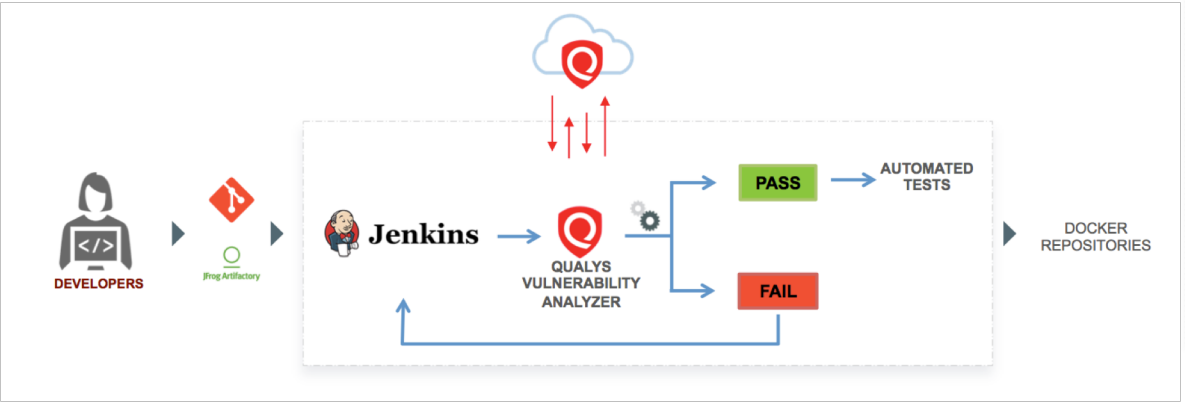
- Image info
- Registry info
- Containers for this image
- Vulnerability posture?
- Easy drill down for complete inventory

Qualys.

Use Case #2

Secure the CI/CD pipeline

Block vulnerable images in the build



Download the **Qualys Vulnerability Analysis plug-in for Jenkins and install** on the Jenkins master

Install the Qualys Container Sensor on the Jenkins worker nodes

Set up policies to Pass/Fail the build. Ex: No Sev.5 vulnerabilities, > CVSS 7, specific QID, vulnerabilities count. Etc.

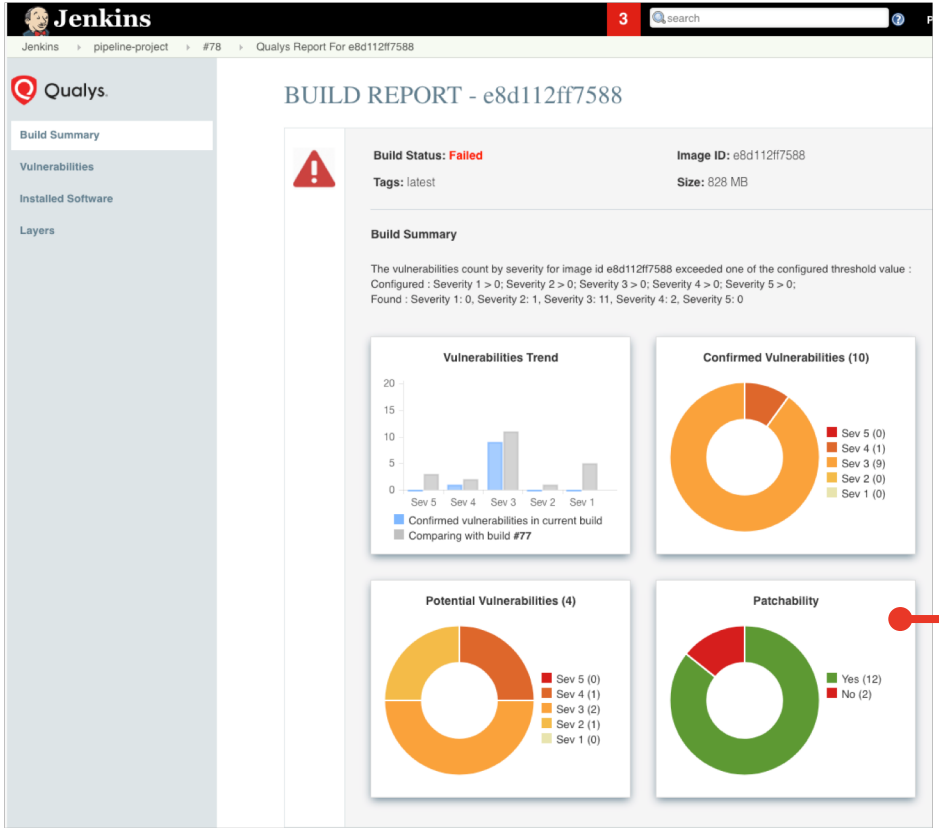
Plugins:

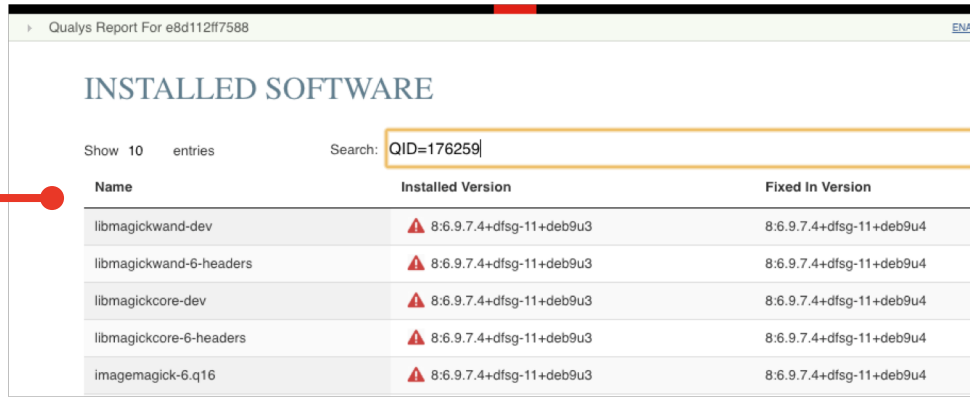
Jenkins Bamboo TC circleci

REST APIs for any other integrations.

*,TeamCity, CircleCI - Support coming soon

Actionable Vulnerability Information





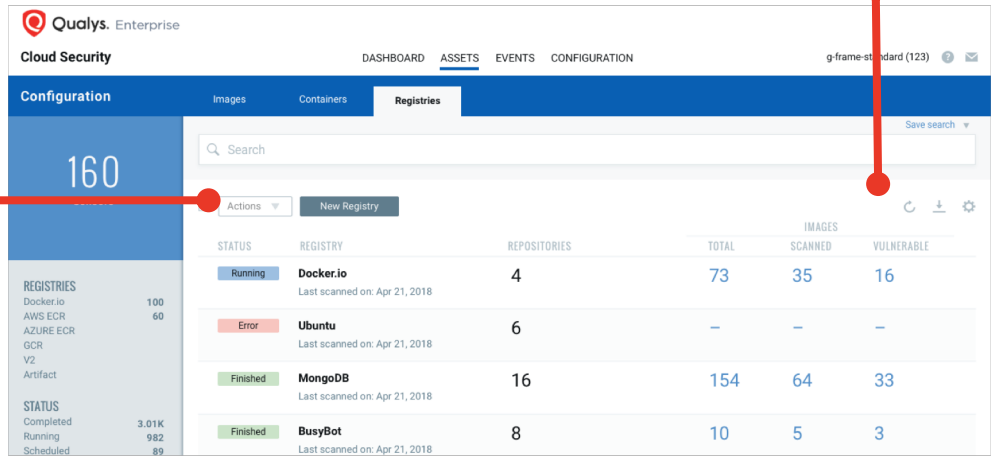
Use Case #3

Scan Registry and block unauthorized images

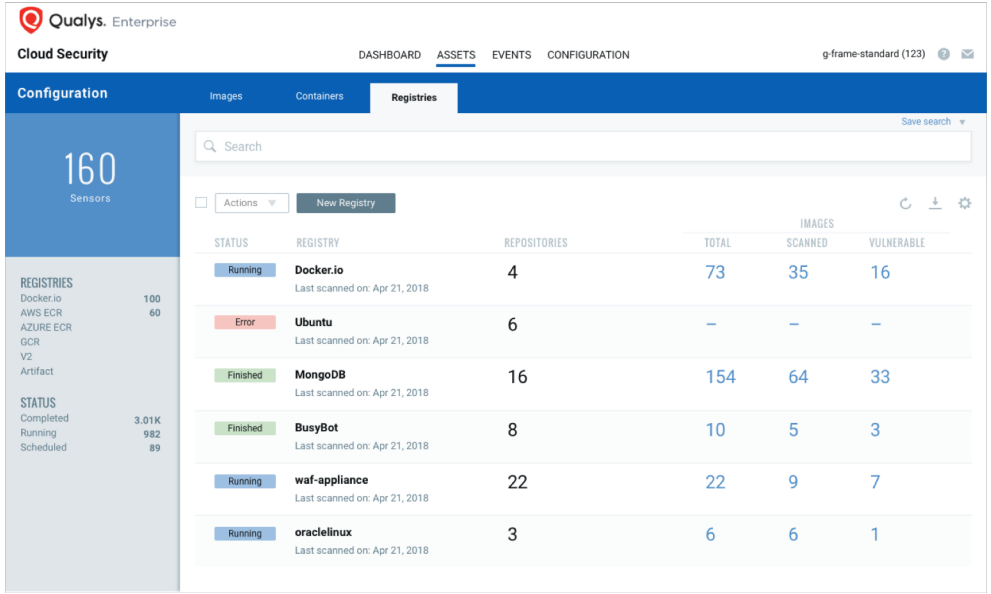
Detect threats from images being shipped

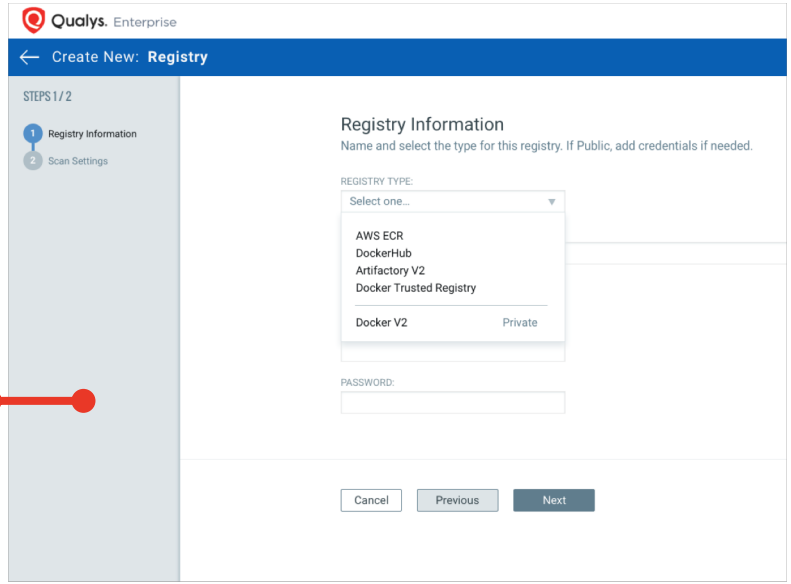
Know your Registries

Vulnerable Images per Registry



Inventory Registry





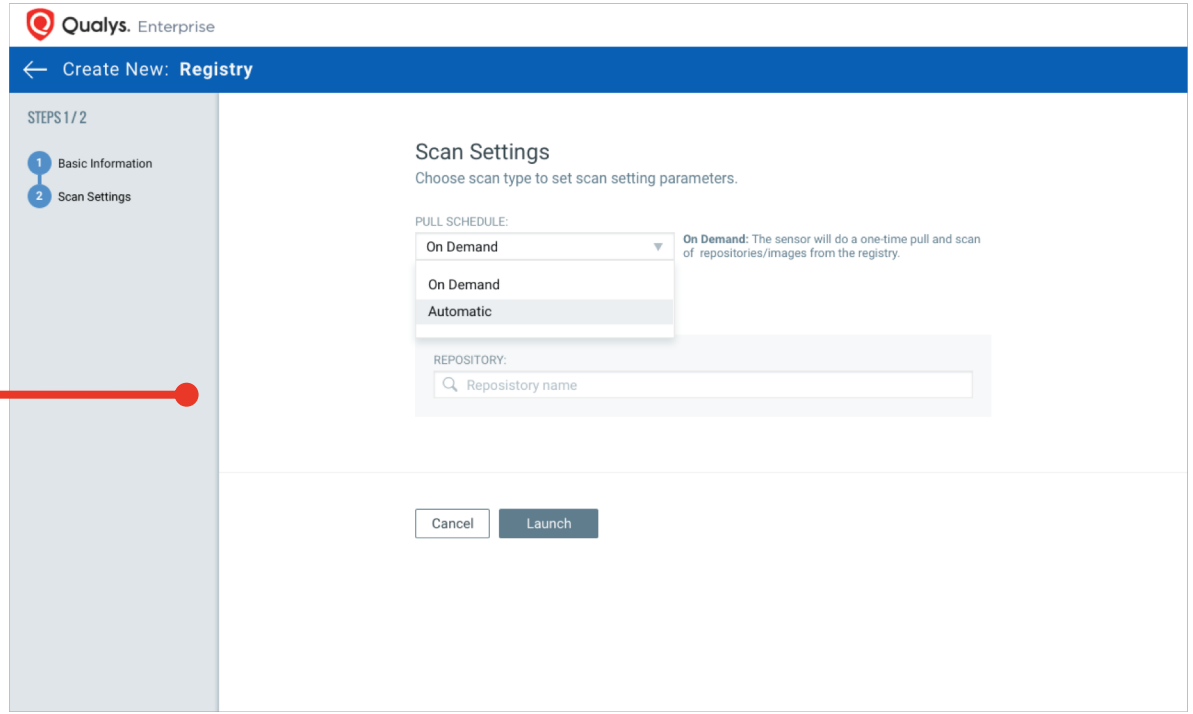
* Support coming soon

Qualys.

Setup Scans

Configure scan frequency for image vulnerability analysis

Automate scanning of images every day at a scheduled time

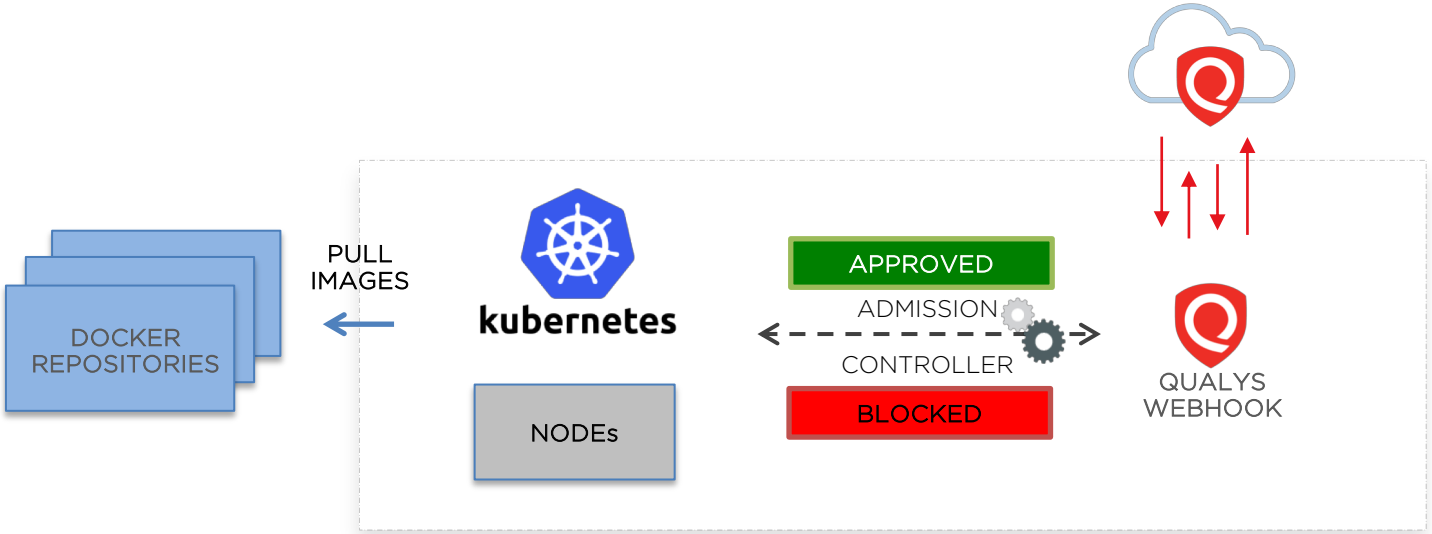


* Support coming soon

Qualys.

Policy based Orchestration

Blocking unapproved images spun up as containers



* Support coming soon

Use Case #4

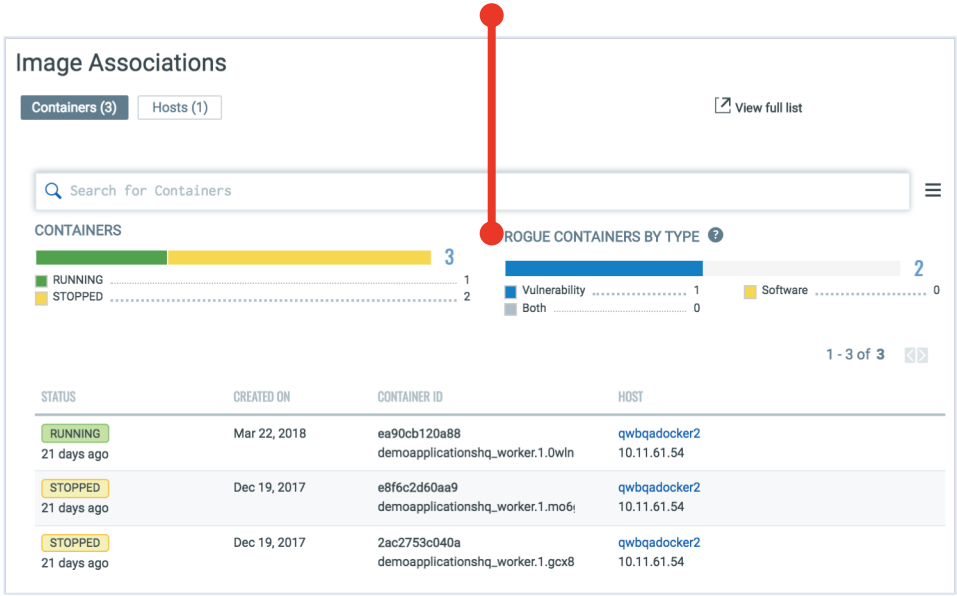
Runtimes Drifts & Protection

Identify potential breaches in containers

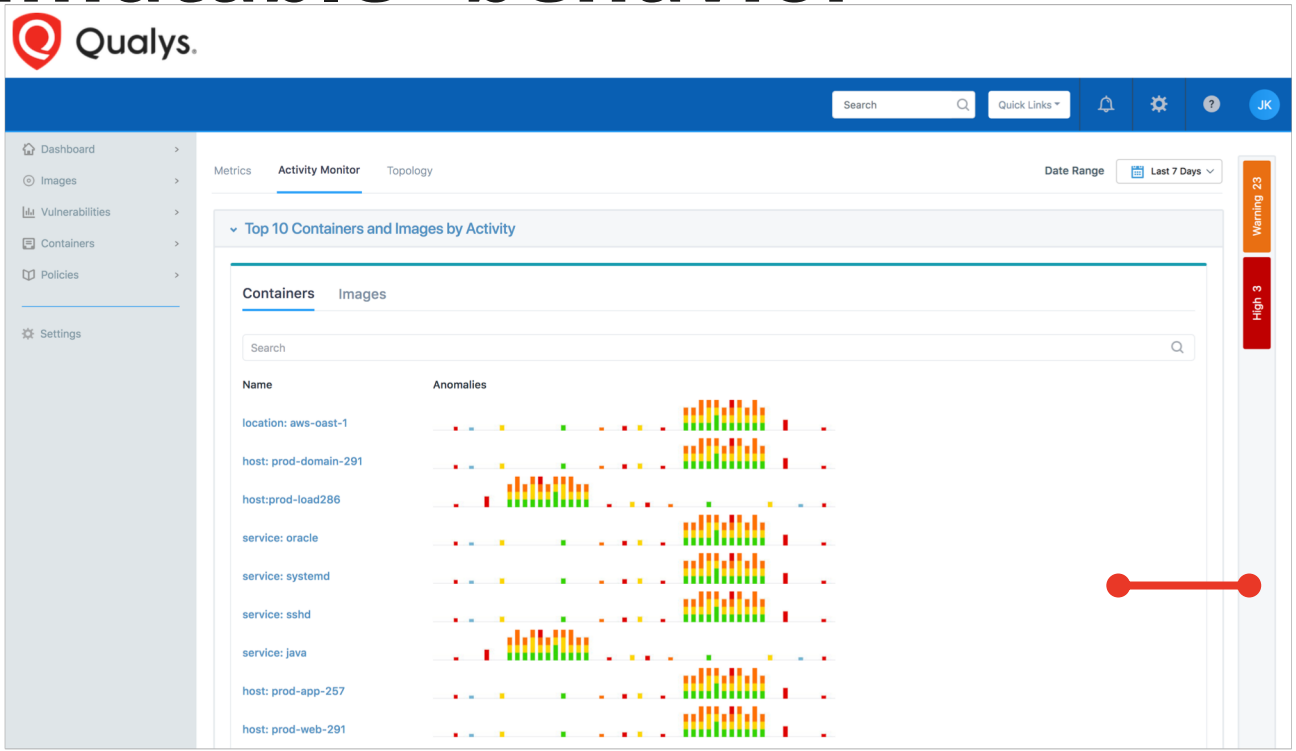
"Rogue" Containers, differ from their parent Images by vulnerability, software package composition, behavior, etc

Detect Containers breaking off from "immutable" behavior

and Block/Kill/Quarantine them.



Containers breaking off from the “immutable” behavior



Drill down to the details,

Identify activity in the containers

Qualys+LI Q3 2019

Qualys.

Qualys.

Search | Quick Links | JK

- Dashboard
- Images
- Vulnerabilities
- Containers
- Policies
- Settings

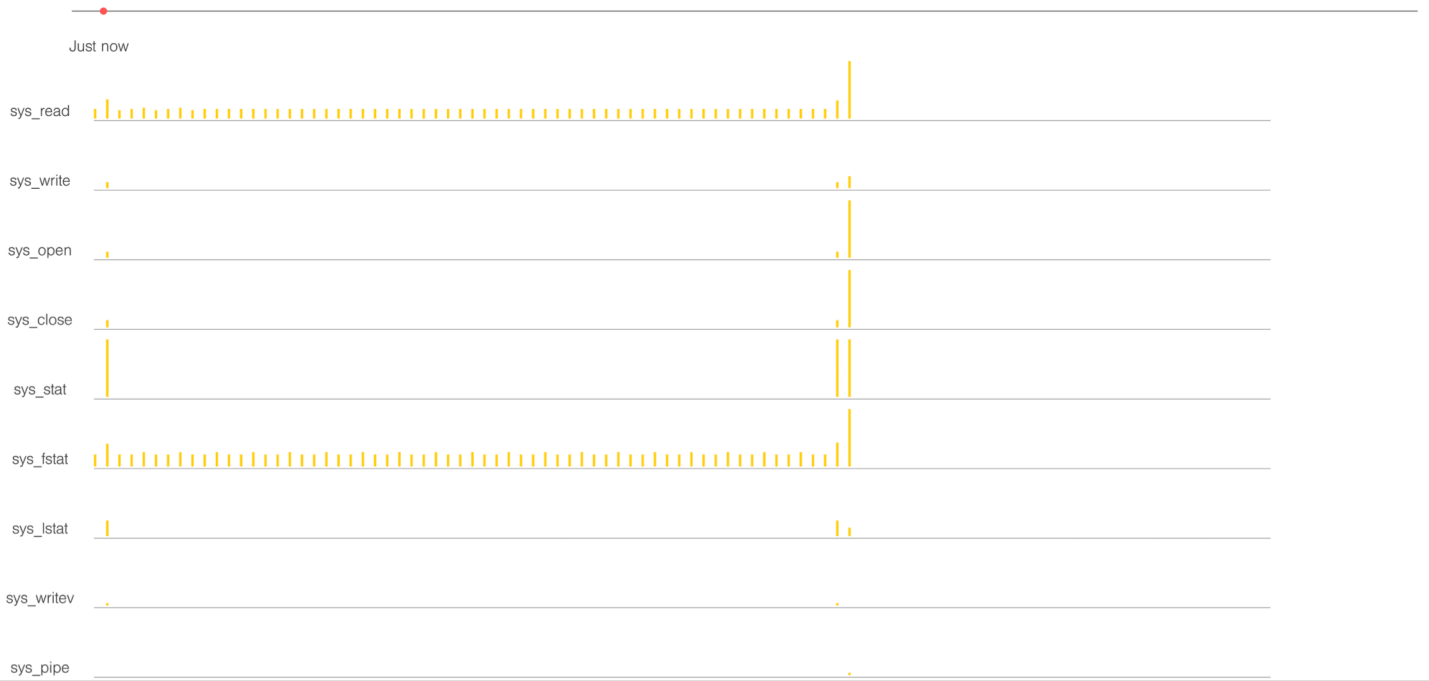
Metrics | **Activity Monitor** | Topology

Date Range: Last 7 Days

Warning 23

High 3

Container Details



Search | Quick Links | JK

- Dashboard
- Images
- Vulnerabilities
- Containers
- Policies
- Settings

Metrics | **Activity Monitor** | Topology

Date Range: Last 7 Days

Warning 23

High 3

Event Details

Process /usr/sbin/httpd was blocked from executing /bin/sh. Severity: High

Raw log:

Process	Process ID	Call	Arguments	Action	Time
/usr/sbin/httpd	31	sys_execve	/bin/sh	Deny	11/13/2018, 12:48:23AM

Processes executing /usr/sbin/httpd:

- /usr/sbin/httpd

Processes accessing /usr/sbin/httpd:

- /usr/sbin/httpd

Qualys Container Security

Host Protection

CIS Benchmarks

Protection for container infrastructure stack

Scanning & Compliance

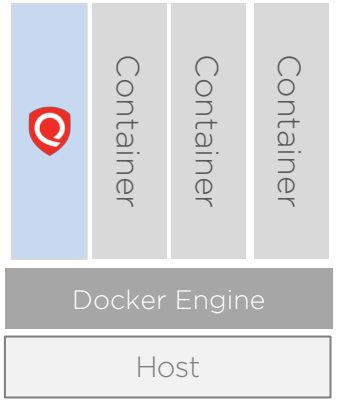
Accurate insight and control of container images

Visibility & Protection

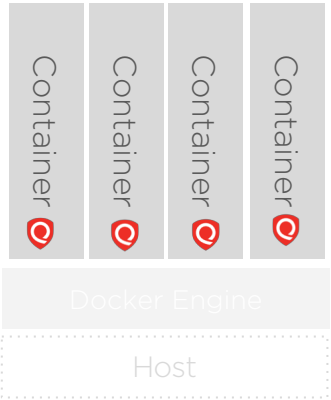
Automated analysis and enforcement of container behavior

Qualys ‘Container Security’ Sensor Options

Qualys Container Sensor
Side-car*



Qualys-Layered Insight
Embedded option

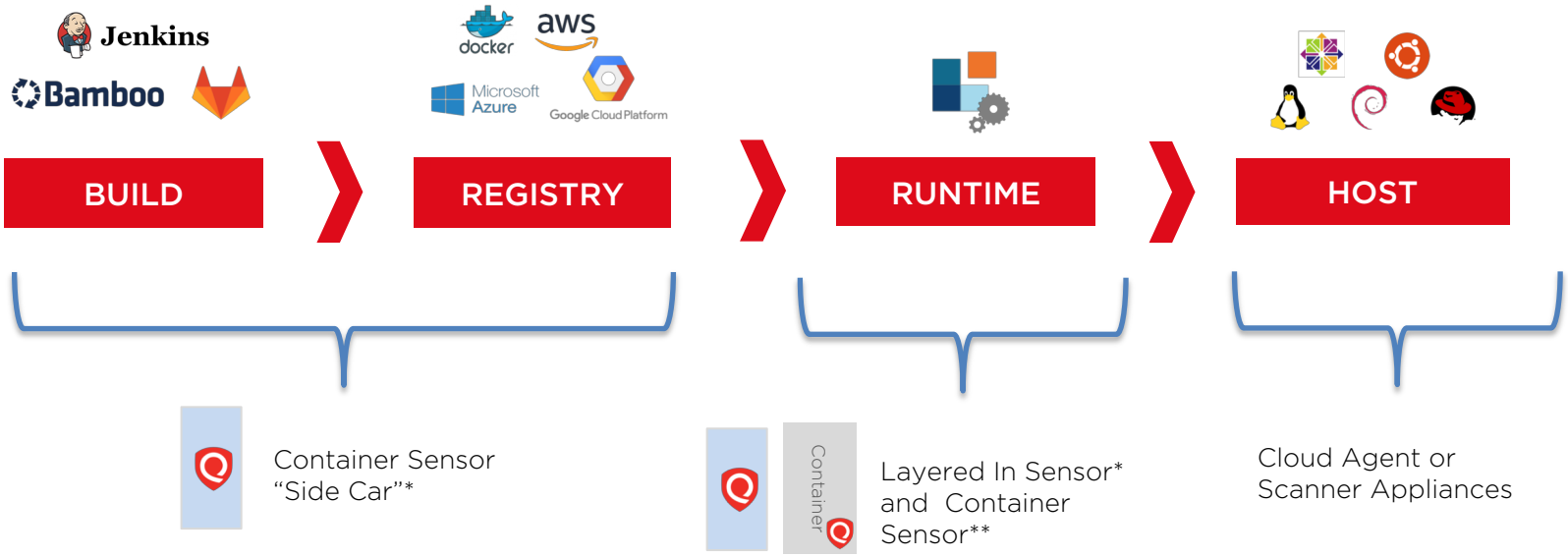


* Qualys side-car to ‘all’ containers on the node. Runs today as non-privileged. As features of compliance and enforcements are added the mode will change to Privileged, with option to revert to non-privileged

Sensors for every use case

PRE-DEPLOYMENT PHASE

POST-DEPLOYMENT PHASE



* Layered In option for runtime protection
** Prevention from starting off malicious containers

Qualys.

Thank You

Hari Srinivasan
hsrinivasan@qualys.com